Executive Office
Office of Information Technology
FY-2007 Service Level Agreement

The **EO/OIT Service Level Agreement** defines the guidelines governing the OD network support services provided by the Office of Information Technology (OIT).

Goals

- Provide dependable, expeditious service and support for the information and technology needs of the OD network users and organizations.
- Promptly respond and resolve problems, account administration and other service requests.
- Consult with OD network users in a dependable and competent manner.
- Standardize configurations and centralize support.

Support Providers

- OIT will provide IT service and support to the OD network users and organizations.
- The NIH Help Desk will receive all requests for OIT technical service and support.

Hours of Service

OIT core hours of service will be 7:00am to 6:00pm on business days. The NIH Help Desk 24x7 web site and the off-hours voicemail serve as the mechanisms for inputting service requests after-hours.

Request for Service and Response Procedures

Non-Emergency Response

- The OD network user will submit all requests for service to the NIH Help Desk by phone on 301-496-4357 (6-HELP), email at Helpdesk@nih.gov , or the Internet at http://support.nih.gov/
- The Help Desk will forward to OIT (within 30 minutes of receipt) an electronic ticket[1] containing the specific information about the request.
- An OIT IT technician will respond to the user within 2 hours after the receipt of the ticket and arrange for the servicing of the request.
    - **Service:** Notify Requester; confirm receipt of ticket.
    - **Timetable:** Within 2 hours
- The technician will periodically update the user on the progress of resolving the issue until the requested service is completed.
- The user can check on the status of an open service request by calling the NIH Help Desk or by using the on-line *Customer Support* web site: http://support.nih.gov/.

[1] This ticket is invaluable to OIT because it provides an audit trail for error tracking, statistical data needed for monitoring service performance of the OIT technicians, and other useful information used to anticipate organizational resources and future information technology (IT) needs of the OD Network.

Emergency Response

If any OD-supported network server experiences an unexpected service outage, OIT will notify those OD network users affected by sending a message via the *OIT News* mailbox or via an NIH Hot News; or, if the users are not able to receive email, OIT will use its *Voice Mail Notification System.*

Services Covered
The OIT will support the following areas:

Problem Resolution
- Troubleshoot and resolve on-site OD network user workstations, supported servers, peripherals and network connectivity.
- Reset your NIH network password.
- Check workstations and servers for security intrusions and malicious software.

Consultation
- Consult on IT support issues and services not specifically identified in this SLA.
- Assist in preparing Statements of Work (SOW) and Memorandums of Understanding (MOU) for IT system projects.
- Serve as a technical advisor on IT contracts.
- Assess users training needs.
- Assess requirements for special customer needs.
- Coordinate with vendors in the implementation of document management systems.
- Provide OD IT orientation to new OD network staff.
- Meet and discuss with administrative officers (AO) services offered by OIT, and identify organization's business rules and requirements.
- Attend AO and organizational staff meetings.
- Advise OD network users concerning hardware and/or software issues.
- Advise OD network users' organizations concerning relocation/office moves.

Workstation Configuration
Install and configure new workstations to OD Desktop Configuration Standards. OD Workstation Configuration
- Configure remote access for laptops and workstations.
- Migrate data between workstations.
- Disassemble and reassemble workstations and/or servers for relocation to other sites.
- Sanitize IT OD and NCMHD-owned equipment to be surplused, transferred, or donated[2].

[2] See *OD ISSO Policy for Sanitizing IT Equipment before Disposal*.

Network Hosting

- Monitor hardware resources, software resources, web servers, databases and supported applications; and analyze performance metrics collected from access and error logs and other technical diagnostics.
    - **Service:** Ensure Network File Server availability during regular business hours.
    - **Timetable:** Provide 97% availability (excludes 4 hours maintenance or utility failure).
- Account management and resource allocation
    - Create, modify, or deactivate OD domain accounts.
    - Create, modify, or deactivate shares, groups, distribution lists, and public folders.
    - Assign file shares.
    - Assign share permissions
    - Create, modify, or deactivate print queues.
- Infrastructure
    - Install, administer, and maintain OD network.
    - Activate existing local-area-network (LAN) outlets.
    - Provide static Internet Protocol (IP) addresses.
- Setup and install new servers
    - Comply with OIT hardware recommendations.
    - Build servers to OIT specifications.
    - Install and tune OS to latest specifications.
- Maintain Internet protocol (IP) subnets.
- Monthly Network Maintenance
    - Perform monthly scheduled maintenance every 3rd weekend.
        - Upgrade infrastructure equipment and/or cabling.
        - Install OS, service packs, hot fixes, security, other server firmware updates, hardware, and/or hardware component
        - Install or update customer requested mission critical applications
    - Send reminder notice to those users, who will be affected by the work on the Wednesday before the performance date.
- Setup and support Windows 2000 and 2003 network print devices.
    - Create print devices at the server level.
    - Support TCP/IP printing on the server level.
- Windows Server 2000 and 2003 Backup and Recovery
    - Perform weekly full and daily incremental data backups and on-demand recoveries/restores.
- Migration Planning and Implementation
    - Migrate user accounts, groups and share objects to new/established servers.
- Host SQL-applications complying with the standard OD network configurations, i.e. the SQL version as stated in the standards and supported by OIT.
- Administer and maintain the system software for OIT-supported Microsoft SQL Servers.
    - Set SQL policies and control of read-only and read/write access to the server.
    - Add, modify, or delete users and groups.
    - Change default property values and create new properties for any system object.
    - Maintain access and error logs.
    - Run activity reports.
    - Create and delete databases.
    - Backup and restore databases.

Web Hosting

- Host Web applications complying with the standard OD network configuration.[3]
- Maintain Microsoft Internet Information Server (IIS) web security configuration and settings.
  - § Set Web policies and control of read-only and read/write access to the server.
  - § Add, modify, or delete users and groups.
  - § Change default property values and create new properties for any system object.
  - § Maintain access and error logs.
  - § Run activity reports.
- Monitor Web Server storage space and, if necessary, inform OD of the need to purchase larger capacity hard drives.
- Windows Server 2000 and 2003 Backup and Recovery
  - § Perform weekly full and daily incremental data backups and on-demand recoveries/restores.

Security

- Comply with DHHS-NIH-OIT system security policies.
- Secure the physical plants i.e., server rooms.
- Provide anti-virus desktop and server support as recommended by OD ISSO.
- Investigate each alert received from CIT Incident Response Team.
- Consult with OD network, application owners per appropriate security levels, practices, etc.
- Assist system owner with contract security language
- Assist system owner with identifying data sensitivity
- Assist system owner with developing system security plan
- Perform a risk assessment of the system
- Identify mitigating measures to reduce the level of risk
- Develop contingency plans for system recovery
- Develop Plan of Action and Milestone POA&M for corrective action
- Assist system owner with filling out the Privacy Impact Statement
- Ensure and certify that the system is operating with an acceptable level of risk
- Request accreditation for system operations
- Develop and keep an electronic versions and hardcopy of documentation that will support the Certification and Accreditation effort.

[3] For non-compliant systems, a separate OD Service Agreement will be required.